ACCEPTABLE USE POLICY

The Internet is a powerful educational resource that can significantly enhance teaching and learning, when used appropriately.

Aoba-Japan International School is committed to providing access to Internet facilities on campus in order to enhance student learning. Vigilance by all members of our school community is required to ensure that students use the internet and digital education resources safely. It is the responsibility of the staff and faculty of Aoba to protect students from harm while at school, including digital environments. It is also the responsibility of Aoba to comply with Japanese Legislation in these areas:

- Protection of Personal Information Act 2017
- Law Banning Child Prostitution and Pornography 2005
- Law on Communications Interception During Criminal Investigations 1999
- Portrait Rights 2005

This policy governs access to and use of the Internet by students of Aoba as well as details, practices, and procedures implemented and carried out by the school and intended to provide maximum protection for users from potential risks associated with the use of the Internet.

The aim of this Acceptable Use Policy (AUP) is to ensure that students will benefit from learning opportunities offered by the school's resources in a safe and effective manner. Internet use and access is considered an Aoba resource and privilege. Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate measures – as outlined in the AUP – will be taken.

Content Filtering, Web Browsing & Downloading

Aoba allows access to millions of websites including games and YouTube, and other similar types of websites, such as blogs but blocks access to websites belonging to categories such as: alcohol, adult content, gambling, and violence.

1. Students will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
2. Students will report accidental accessing of inappropriate materials in the classroom to their teacher.
3. Students are encouraged to report accidental access of inappropriate materials in school but outside the classroom to their homeroom teacher.
4. Students will not copy information from the internet without acknowledging the creator and referencing the source of the content.
5. In principle, students will use the Aoba internet connection only for educational and career development activities.

E-mail & Messaging

Online communication through a student's assigned email account is mandatory. The use of personal email accounts on campus is not acceptable.

1. Students should not under any circumstances share their email account login details with other students.

2. Students will not send any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
3. Students should avoid opening emails that appear suspicious.
4. If in doubt, students should ask their teacher before opening emails from unknown senders.
5. When using peer-to-peer messaging such as Google Hangouts, all behavioural expectations that apply in all school situations apply equally here, whether before, during, or after the school day.

BYOD & Mobile Phones

The bring your own device (BYOD) program allows students to bring their own Apple laptop or iPad to school to support teaching and learning activities.

1. Students take responsibility for appropriate use of their personal device at all times. The school is not responsible in any way for personal devices or for its use.
2. Students/parents/guardians are responsible for their devices, including any breakages, costs of repair, or replacement.
3. The school reserves the right to inspect devices during school hours.
4. Violations of any school policies or rules involving a student device may result in a student not being allowed to continue using the device during school hours and/or disciplinary action, for a period to be determined by the school.
5. During school hours, students are allowed to use their device for learning related activities only.
6. Students must comply with teachers' requests regarding use of devices during school hours, and classes.
7. Students may not use the devices to record, transmit or post photos or video of other teachers or students. No images or video recorded at school can be transmitted or posted at any time without their teacher's permission.
8. Students may use the school wireless network and content filtered broadband. Use of other 'unfiltered' public wireless connections, such as mobile networks, is not allowed during school hours.
9. Each user is responsible for her/his own device and should use it responsibly and appropriately. Aoba takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices.
10. Aoba is not responsible for any possible device charges to their account that might be incurred during approved school-related use.
11. Teachers may confiscate devices until the end of the school day if the teacher observes the student using the device for non-school-related purposes.

Images & Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

1. Staff, parents/guardians and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide opportunities for harassment or breaches of privacy to take place. Digital images may remain available on the internet forever and may cause harm to individuals in the short or longer term.
2. Care should be taken when taking photographic or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
3. At Aoba, students must not take, use, share, publish or distribute images of others without their permission.
4. Taking photos or videos on the grounds of Aoba or when participating in school activities is only allowed with express permission from staff.
5. Students must not share images, videos or other content online with the intention to harm another member of the Aoba community regardless of whether this happens in school or outside. Sharing explicit images and in particular explicit images of students and/or minors is an unacceptable (illegal) and absolutely prohibited behaviour, with serious consequences for those involved. Sharing explicit images of other students automatically incurs suspension as a consequence.

Cyberbullying

This type of bullying is increasingly common and is continuously evolving. It is bullying carried out through the use of information and communication technologies such as text, social networking sites, e-mail, instant messaging, apps, gaming sites, chat-rooms and other online technologies.

1. Being the target of inappropriate or hurtful messages is the most common form of online bullying. As cyberbullying uses technology to perpetrate bullying behaviour and does not require face-to-face contact, cyberbullying can occur at any time (day or night).
2. Many forms of bullying can be facilitated through cyberbullying. For example, a target may be sent homophobic text messages or pictures may be posted with negative comments about a person's sexuality, appearance, ethnicity, etc.
3. Students are increasingly communicating in ways that are often unknown to adults and free from supervision. The nature of these technologies means digital content can be shared and seen by a very wide audience almost instantly and is almost impossible to delete permanently. While cyberbullying often takes place at home and at night, the impact can also be felt in school.
4. Cyberbullying is defined as repeatedly engaging in online activities with the intent to harm, harass, or embarrass another student or member of staff. It is an unacceptable and absolutely prohibited behaviour, with serious consequences for those involved.

How does Aoba ensure a safe digital learning environment?

1. At Aoba-Japan International School, the digital safety and security of our students is of utmost importance.
2. Using modern network infrastructure and filtering solutions, our ICT Engineers ensure the safety of the school's internal network.
3. Additionally, all of our staff and faculty are trained in safe, responsible internet usage and put these skills into practice during educational activities.
4. All of our teachers are Google Certified Educators and many are Apple Distinguished Educators, recognised as global leaders in Digital Literacy and Educational Technology.

Important points:

1. Aoba ICT does not control what content students access at an individual level.
2. Aoba ICT does not install software and configure parental controls on student devices.
3. Aoba Faculty are expected to monitor device and internet usage within the classroom.
4. Parents are expected to monitor device and internet usage outside of school.
5. Our filtering policies are reviewed and approved by school leadership. We can schedule a review and adjustment of our filtering policies at any time.

Network Access and Security

1. Aoba campuses utilise powerful Firewall devices which allow specific control over anti-virus, threat protection, and filtering on the school network.
https://www.cyberoam.com/webfiltering.html
2. Our Firewall prevents access to inappropriate or potentially harmful content related to drugs, firearms, adult content and more.
3. Furthermore, students only have access to the internet at school via the Aoba Student network. This network falls under the security and filtering protections provided by our Firewall devices.
4. Students must be enrolled into our MDM (mobile device management) system in order to use this.
5. If they are not, they can not access the internet at Aoba.
https://meraki.cisco.com/solutions/mobile-device-management

Parental Controls

Parental controls are not mandated by the school.

We encourage parents to carefully consider what protections and restrictions should be placed on their child's device based on their child's age and their own family values.

There are several options for applying Parental Controls to a student's device:

macOS Parental Controls / ペアレンタルコントロール

English: https://support.apple.com/kb/PH25799?locale=en_US

日本語: https://support.apple.com/kb/PH25799?locale=en_US&viewlocale=ja_JP

macOS Monitor Computer Usage / コンピュータの使用を監視する

English:
https://support.apple.com/guide/mac-help/monitor-childrens-computer-usage-mchlp2911/mac

日本語:
https://support.apple.com/ja-jp/guide/mac-help/monitor-childrens-computer-usage-mchlp2911/mac

iOS Parental Controls / 機能制限を使う

English: https://support.apple.com/en-us/HT201304

日本語: https://support.apple.com/ja-jp/HT201304

Third-party apps and software solutions for parental control:

Apple以外のソリューション:

https://screentimelabs.com/

https://kidslox.com/en/

http://ourpact.com/

Predominantly drawn from:
https://s3-eu-west-1.amazonaws.com/client-castleknockcc/wp-content/uploads/2013/07/AUP-2017-2020.pdf

Other examples:

https://www.k12blueprint.com/sites/default/files/Acceptable-Use-Policies.pdf

http://mercyinchicore.ie/drupal-7.15/node/47

For questions, comments or concerns relating to the Aoba-Japan International School ICT Acceptable Use Policy please contact the Aoba Department at **ict@aobajapan.jp**

Adopted: 2019
Leadership Reviewed: 12 Dec 2023
Faculty Reviewed: 13 Dec 2023
Leadership Approved: